

Khamis, M., Alt, F., Hassib, M., von Zezschwitz, E., Hasholzner, R. and Bulling, A. (2016) GazeTouchPass: Multimodal Authentication Using Gaze and Touch on Mobile Devices. In: CHI EA '16: 34th Annual ACM Conference Extended Abstracts on Human Factors in Computing Systems, San Jose, CA, USA, 07-12 May 2016, pp. 2156-2164. ISBN 9781450340823.

There may be differences between this version and the published version. You are advised to consult the publisher's version if you wish to cite from it.

© The Authors 2016. This is the author's version of the work. It is posted here for your personal use. Not for redistribution. The definitive Version of Record was published in the Proceedings of the 34th Annual ACM Conference Extended Abstracts on Human Factors in Computing Systems, San Jose, CA, USA, 07-12 May 2016, pp. 2156-2164. ISBN 9781450340823
<https://doi.org/10.1145/2851581.2892314>.

<http://eprints.gla.ac.uk/170228/>

Deposited on: 5 October 2018

GazeTouchPass: Multimodal Authentication Using Gaze and Touch on Mobile Devices

**Mohamed Khamis¹, Florian Alt¹, Mariam Hassib^{1,2},
Emanuel von Zezschwitz¹, Regina Hasholzner¹, Andreas Bulling³**

¹ Media Informatics Group, University of Munich (LMU), Munich, Germany
{mohamed.khamis, florian.alt, mariam.hassib,
emanuel.von.zezschwitz}@ifi.lmu.de, hasholzner@cip.ifi.lmu.de

² VIS, University of Stuttgart, Stuttgart, Germany
mariam.hassib@vis.uni-stuttgart.de

³ Perceptual User Interfaces Group, Max Planck Institute for Informatics, Saarbrücken, Germany
bulling@mpi-inf.mpg.de

Permission to make digital or hard copies of part or all of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for third-party components of this work must be honored. For all other uses, contact the Owner/Author. Copyright is held by the owner/author(s).

CHI'16 Extended Abstracts, May 07-12, 2016, San Jose, CA, USA ACM
978-1-4503-4082-3/16/05. <http://dx.doi.org/10.1145/2851581.2892314>

Abstract

We propose a multimodal scheme, GazeTouchPass, that combines gaze and touch for shoulder-surfing resistant user authentication on mobile devices. GazeTouchPass allows passwords with multiple switches between input modalities during authentication. This requires attackers to simultaneously observe the device screen and the user's eyes to find the password. We evaluate the security and usability of GazeTouchPass in two user studies. Our findings show that GazeTouchPass is usable and significantly more secure than single-modal authentication against basic and even advanced shoulder-surfing attacks.

Author Keywords

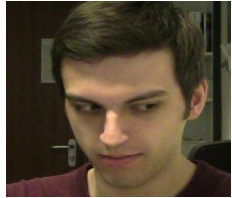
Multimodal Authentication; Gaze Gestures; Mobile Devices

ACM Classification Keywords

H.5.2 [Information Interfaces and Presentation]: User Interfaces; K.6.5 [Computing Milieux: Security and Protection]: Authentication

Introduction

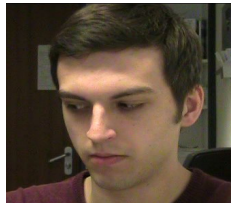
With mobile devices enabling ubiquitous access to sensitive information, there is a need to protect access to such devices. Meanwhile, authentication schemes are prone to shoulder-surfing attacks [20], where a bystander observes a user while authenticating. The attacker then gets hold of the device and tries to authenticate and access sensitive data.



Gaze (Left)



Touch (3)



Gaze (Right)



Touch (4)

Figure 1: GazeTouchPass uses gaze and touch for authentication on smartphones. This requires attackers to observe both the user’s eyes and the touchscreen.

Recent work proposed schemes that are more resistant to observations [11, 25]. However in most cases, attacking state of the art schemes involves observing only one entity – the phone – in preparation for an attack.

At the same time high-resolution front-facing cameras made it possible to track users’ gaze on mobile devices [12, 13, 14, 21, 27]. These advances took gaze-based authentication from desktop systems [4, 5, 16], to mobile devices [17]. This work combines gaze and touch input for secure user authentication on off-the-shelf mobile devices.

We propose a novel multimodal scheme, GazeTouchPass, that makes mobile user authentication more robust against shoulder-surfing by requiring attackers to simultaneously observe both the user’s eyes and the phone (Figure 1). GazeTouchPass combines gaze and touch input into multimodal passwords (e.g. left-3-right-4).

The contributions of this work are two-fold. First, we introduce the concept and the implementation of GazeTouchPass, a novel multimodal authentication scheme that secures mobile devices against classic and even advanced shoulder-surfing attacks. Second, we report on an evaluation of the system’s usability and security, and compare it to state-of-the-art schemes. Our findings show that multimodal authentication using gaze and touch is significantly more secure than single-modal authentication against basic and even advanced shoulder-surfing attacks.

Threat Models

GazeTouchPass addresses two threat models, in both models the user is in a public space that is not under the control of the attacker. The attacker is familiar with the system and knows how to provide a password.

Iterative attacks. The attacker can observe the user several times (e.g. a colleague at work) from different viewpoints. The attacker exclusively focuses on one modality per observation – on the users’ eyes (eyes-view) and then on the input on the screen (phone-view), or vice versa. The challenges of this attack are to (a) correctly remember both sequences and to (b) correctly combine them later.

Side attacks. The attacker observes the user while authenticating once (e.g. in a subway) from an angle that allows the user’s eyes as well as the user’s input on the touch screen to be observed. The distance between the attacker and the user is close enough to see the touchscreen, but far enough to reduce the effort of switching focus back and forth between the user’s eyes and the device’s display.

GazeTouchPass: Multimodal Passwords

Based on these threat models we propose GazeTouchPass, a multimodal authentication scheme in which users define four symbols, each can be entered either via touch (a digit between 0 and 9) or via gaze (gazing to the left and to the right). Consecutive gaze inputs to the same direction would then need to be separated by a gaze to the front.

We expect that the more switches between input modalities are used within a single password, the more difficult it will be to observe it. For example, we expect: “1-left-2-right” (3-switches) to be more secure than “1-2-left-right” (1-switch). As for side attacks, each switch in input modality is equivalent to a switch of the attacker’s focus between the touchscreen and the eyes. In case of iterative attacks, as switches between modalities increase, so do the possible combinations of observations from the eyes-view and the phone-view. Examples of passwords with different number of modality switches are shown in Table 1.

Condition	Examples
0-switches (<i>baseline</i>)	1-2-3-4 left-right-left-left
1-switch	left-1-2-3 1-2-left-right
2-switches	left-1-left-right left-1-2-right
3-switches	1-left-2-right left-1-right-2

Table 1: We studied the effect of the number of switches between gaze input and touch input. It is expected that the more switches between modalities a password has, the more resistant it is to shoulder-surfing. A password with 0-switches in input modalities is considered the baseline as it represents a single modal password consisting of either digits only or gaze gestures only.

The login interface consists of 10 buttons similar to a common 10-digit keypad (see Figure 1). Users log in by touching digits and moving their eyes. The system is implemented as an Android application and does not require any additional hardware. The user’s face and eyes are first detected using the Viola-Jones detector [24] through the device’s front-facing camera. On top we then use a calibration-free gaze estimation approach similar to a method recently introduced for interaction with public displays [28]. Our method calculates the distance between the center of the face and the pupil for each eye. Discrete gaze directions are then estimated based on the ratio between both distances.

Usability Study

The aim of this study is to analyze the usability of Gaze-TouchPass and to collect video recordings of gaze and touch input for the subsequent security study. In a repeated measures experiment, each participant performed 16 authentications ($4 \text{ passwords} \times 4 \text{ conditions}$) using randomly generated passwords. We recruited 13 participants (9 females), aged between 21 and 35 years ($M = 25.23$, $SD = 3.8$). We logged all login attempts and recorded the participants using three HD video cameras (see Figure 2).

Each participant performed a training run per condition, to get acquainted with the system. These runs were excluded from further analyses. At each authentication attempt, the experimenter read out the password to be entered according to a previously generated, randomized list. Participants repeated entry in case of false login. The study was concluded with a semi-structured interview. We evaluated the system’s usability based on input speed and error rate.

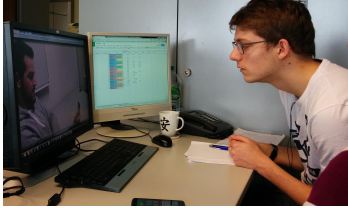
Input Speed. We measured the time taken to input the passwords. We excluded 3 out of 72 input time measurements prior to analysis as outliers ($> \mu + 3 \times SD$). No



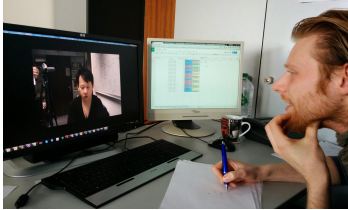
Figure 2: The usability study setup. Cameras A and B simulate an iterative attack (observing the phone screen and user’s eyes separately), while Camera C simulates a side attack (observing the phone screen and user’s eyes simultaneously).

significant main effects were found for number of modality switches on authentication time ($p > 0.05$). Figure 3 suggests that mean authentication times do not vary greatly among different number of modality switches.

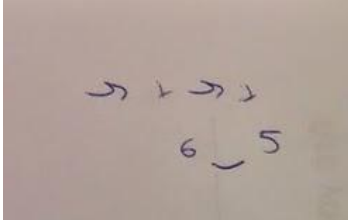
Error Rate. We also logged the number of failed login attempts, which were either due to incorrect input or false detection by the system. A Pearson chi-square test showed no significant effect of number of modality switches on error rate $\chi^2(30) = 33, p = 0.32$. Figure 5 shows that there were fewer errors in the case of passwords with 3-switches. While providing multiple consecutive gaze gestures can be error prone, having 3 switches in a 4-digit password can be achieved only by alternating gaze gestures and digits.



(a)



(b)



(c)

Figure 4: (a) A participant observing the side-view during a side attack. (b) A participant observing the eyes-view as part of an iterative attack. (c) When performing iterative attacks, participants noted the pauses between gaze gestures then tried to fill the gaps with digits observed through the phone-view.

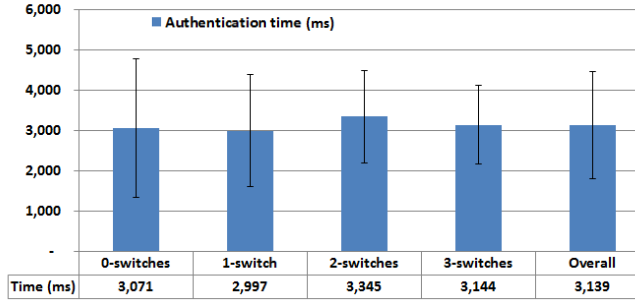


Figure 3: Mean authentication times for passwords with different numbers of modality switches. Authentication times do not vary significantly among different number of modality switches. Overall mean authentication time is 3.1 seconds ($SD=1.3$).

Qualitative Feedback. Six out of 13 participants reported they would use GazeTouchPass as a primary authentication scheme. Nine reported that they would not use it for daily unlocking, but rather for insecure situations or to protect sensitive data, such as their online banking apps. One participant indicated that she would be willing to use GazeTouchPass for a one-time unlock (e.g. when switching the phone on). Four participants said they would not be willing to do anything extra for higher security; two of them added that they do not use any lock mechanism on their phones.

Security Study

In the security study, we used the videos recorded from the preceding study to evaluate the security of GazeTouchPass. Following a repeated measures design, participants attacked passwords with all four possible number of switches and observed from all views using the videos recorded during the usability study. Every participant attacked 8 passwords of each condition of n -switches – half of which were side attacks (side-view), while the others were iterative attacks (phone-view and eyes-view) where the experimenter alternated the order of the observed view. Each participant

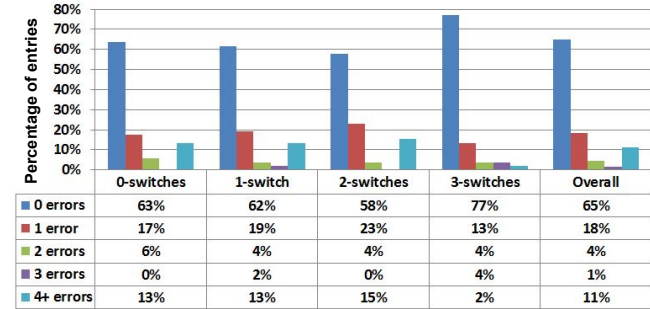


Figure 5: Number of attempts before a successful entry. Errors are less for passwords with 3-switches; consecutive gaze gestures can be error prone, while 3-switches in an $n=4$ password can be only achieved by alternating gaze and touch input.

attacked 32 passwords. The order of videos was randomized per participant. To avoid learning effects, no participant attacked the same password from different views.

We recruited 13 participants (6 females), aged between 21 and 33 years ($M = 24.2$, $SD = 3.4$), through mailing lists, none of whom had participated in the usability study. Participants were compensated with a 10 Euro voucher. In addition, all participants took part in a draw for an additional 20 Euro voucher, where chances of winning increased with the number of successfully attacked passwords.

The experimenter introduced the study procedure, the task, and the rewarding mechanism. After explaining the system, participants had the chance to try and get acquainted with the app themselves. They were given draft papers, then the experimenter started playing the videos. Based on their observations, participants provided up to three guesses (Figure 6). The study was concluded with a questionnaire and a semi-structured interview. In total, participants performed $13 \times 32 = 416$ attacks with up to three guesses each.

System	Login time
GazeTouchPass	
3-switches	3.1s
2-switches	3.3s
1-switches	3.0s
0-switches	3.0s
EyePassShapes [6]	12.5s
EyePIN [8]	48.5s
CGP [10]	36.7s
EyePassword [16]	9.2s-12.1s
Liu et al. [17]	9.6s
PhoneLock [1]	12.2s - 28.2s
SpinLock [2]	10.8s - 20.1s
TimeLock [3]	10s
ColorLock [3]	10s
XSide [7]	
front 1-switch start	3.9s
front 1-switch end	3.7s
front 2-switches	3.8s
back 1-switch start	3.8s
back 1-switch end	4.1s
back 2-switches	4.0s

Table 2: Authentication times using GazeTouchPass compared to state-of-the-art schemes that use gaze-based authentication [6, 8, 10, 16, 17], input-splitting (e.g. XSide [7]) and multiple modalities [1, 2, 3].

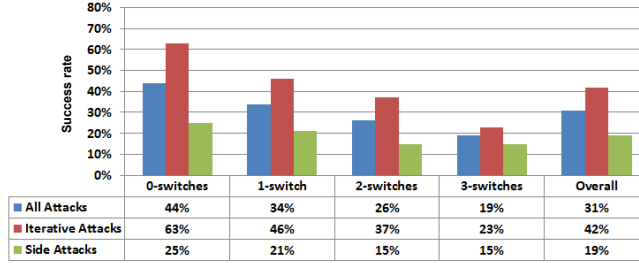


Figure 6: Success rate when attacking passwords entered using GazeTouchPass. The more switches in input modality per password, the less likely it is successfully attacked. Side attacks are always less successful than iterative attacks due to the difficulty of continuously switching focus back and forth from the eyes to the touchscreen.

Successful Attacks. For every attack we calculated the Levenshtein distance between the guesses and the correct password. Only the guess closest to the correct password was considered for further analysis. Moreover, we calculated the overall success rate in attacking passwords for each number of modality switches and for each attack type (iterative attack vs side attack). An attack is successful if at least one guess matched the correct password. Figure 6 summarizes the successful attack rate against passwords with different number of modality switches, observed through the side-view or through the phone-view and the eyes-view.

A repeated measures ANOVA showed significant main effects for number of modality switches on attack success ($F_{3,36} = 3.86, p < 0.05$). This suggests that distance between the guesses and the correct password depends on the modality switches. Post-hoc analysis using Bonferroni correction showed a significant difference ($p < 0.05$) in attack success for passwords with 0-switches ($M = 1.25, SD = 0.14$) compared to those with 3-switches ($M = 1.9,$

$SD = 0.1$). This means guesses against passwords with 0-switches in modality (baseline) are closer to the correct pattern than those with 3-switches. The other pairs did not show any significant differences ($p > 0.05$).

There were significant main effects for the view angle on attack success ($F_{1,12} = 51.05, p < 0.0001$). No interaction effects were found between the number of modality switches and the view angle ($p > 0.05$). Post-hoc analysis using Bonferroni correction revealed that there was a significant difference ($p < 0.0001$) in attack success for passwords attacked iteratively ($M = 1.38, SD = 0.138$) compared to passwords attacked from the side ($M = 1.913, SD = 0.123$). This suggests that guesses against passwords observed iteratively are closer to the correct password compared to those observed from the side.

Qualitative Feedback. When asked how easy it was to attack passwords for each view (5-point Likert scale; 1=Very easy; 5=Very difficult), participants found side attacks to be very difficult ($Med = 5, SD = 0.66$), while iterative attacks were perceived to be easier ($Med = 3, SD = 0.96$). Eight participants expressed that attacking touch-only and gaze-only passwords were easiest. One participant reported it was easier to break passwords with consecutive inputs of the same modality. There was a disagreement among participants in which modality it was more difficult to observe. While some found gaze input to be more difficult to observe than touch input, others found gaze-input easier. Participants reported side attacks to be harder as it was difficult to concentrate on the eyes and the display at the same time. Three participants said that they had trouble finding the right order during iterative attacks. They also reported that it is harder to attack passwords entered quickly. It is expected that users will login faster as they use the system more often, making the system even more secure.

System	Successful attacks
GazeTouchPass	
3-switches (Side)	15%
3-switches (Iterative)	23%
2-switches (Side)	15%
2-switches (Iterative)	37%
1-switches (Side)	21%
1-switches (Iterative)	46%
0-switches (Side)	25%
0-switches (Iterative)	63%
EyePassShapes [6]	42%
EyePIN [8]	55%
XSide [7]	
front 1-switch start	38%
front 1-switch end	13%
front 2-switches	28%
back 1-switch start	19%
back 1-switch end	16%
back 2-switches	9%

Table 3: Successful attack rates using GazeTouchPass compared to state-of-the-art schemes that use gaze-based authentication [6, 8] and input-splitting (e.g. XSide [7]). Some relevant systems were excluded from this table as their security was not evaluated in a way comparable to our studies [1, 2, 3, 10, 16, 17].

Discussion

GazeTouchPass is particularly secure against side attacks (only 15%-21% success rate). Iterative attacks are complicated but possible in optimal conditions (23%-46%), given that the adversary paid attention to all inputs and noted the gaps between them (see Figure 4c). It should be noted that we assume the attacker knows how the observed system works. The proposed threat models are realistic yet ensure optimal conditions. Nevertheless, GazeTouchPass is more secure than most comparable systems (see Table 3).

Mean authentication time using GazeTouchPass is approximately 3.1 seconds. While this is slower than less secure schemes (von Zezschwitz et al. [26] report 1.5 seconds for PINs and 3.13 seconds for patterns), GazeTouchPass is faster than security-optimized state-of-the-art authentication systems (see Table 2). Overall, and as several participants indicated, GazeTouchPass can be particularly useful as a secondary authentication mechanism that users can choose to opt to when feeling observed (e.g. public setting), or when accessing critical data (e.g. online banking).

GazeTouchPass achieves a balance between security and usability, with low authentication times and high observation resistance. Tables 2 and 3 show that it is faster and more secure than gaze-based schemes [6, 8, 10, 16]. Comparing GazeTouchPass to mobile-based schemes that use multiple modalities, we found that although the security of PhoneLock [1], SpinLock [2], TimeLock [3], ColorLock [3] and the system by Liu et al. [17] was not evaluated in a way comparable to our studies, our system requires shorter login times (see Table 2), and uses a higher password space (12^n) than that of [17]. XSide [7] splits the input using a double-sided touchscreen. Still GazeTouchPass is faster and can work on off-the-shelf mobile devices without additional hardware. Similarly, the number of switches in an XSide

password influences its security; in most cases GazeTouchPass is more resistant to observations (see Table 3).

Limitations and Future Work

While GazeTouchPass shows that multimodal passwords are significantly more secure than single-modal ones, iterative attacks are still possible and perceived to be relatively easy to perform. Future work should focus on increasing resistance to iterative attacks while maintaining usability. One possible approach is to introduce a random cue [19] to the user that would complicate attempts to combine observations from multiple views. We will also study the memorability and practical password space of GazeTouchPass.

Video-based eye tracking has its known limitations; varying light conditions, reflections of eye glasses and heavy makeup can affect the quality of eye tracking [18]. For this reason we opted for simple eye gestures that can be robustly detected by frontal-cameras. However, the use of better eye tracking equipment (e.g. infrared light sources and sensors) can enable a wider range of eye movements to be detected robustly. Future systems can use different types of eye movements. For example, the smooth pursuits eye movement has recently gained attention in enabling calibration-free gaze-based interaction [5, 9, 15, 22, 23].

Conclusion

In this paper we introduced multimodal authentication combining gaze and touch on mobile devices. GazeTouchPass is significantly more secure than single modal systems, particularly against side attacks due to having to quickly switch focus between phone and eyes. Its usability compares favourably to state-of-the-art schemes. Our conclusion is that the use of multiple modalities can greatly enhance the security of authentication systems against advanced as well as basic threat models, while maintaining high usability.

References

- [1] Andrea Bianchi, Ian Oakley, Vassilis Kostakos, and Dong Soo Kwon. 2011. The Phone Lock: Audio and Haptic Shoulder-surfing Resistant PIN Entry Methods for Mobile Devices. In *Proceedings of the Fifth International Conference on Tangible, Embedded, and Embodied Interaction (TEI '11)*. ACM, New York, NY, USA, 197–200. DOI : <http://dx.doi.org/10.1145/1935701.1935740>
- [2] Andrea Bianchi, Ian Oakley, and DongSoo Kwon. 2011. Spinlock: A Single-Cue Haptic and Audio PIN Input Technique for Authentication. In *Haptic and Audio Interaction Design*, EricW. Cooper, VictorV. Kryssanov, Hitoshi Ogawa, and Stephen Brewster (Eds.). Lecture Notes in Computer Science, Vol. 6851. Springer Berlin Heidelberg, 81–90. DOI : http://dx.doi.org/10.1007/978-3-642-22950-3_9
- [3] Andrea Bianchi, Ian Oakley, and Dong Soo Kwon. 2012. Counting clicks and beeps: Exploring numerosity based haptic and audio {PIN} entry. *Interacting with Computers* 24, 5 (2012), 409 – 422. DOI : <http://dx.doi.org/10.1016/j.intcom.2012.06.005>
- [4] Andreas Bulling, Florian Alt, and Albrecht Schmidt. 2012. Increasing the Security of Gaze-based Cued-recall Graphical Passwords Using Saliency Masks. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '12)*. ACM, New York, NY, USA, 3011–3020. DOI : <http://dx.doi.org/10.1145/2207676.2208712>
- [5] Dietlind Helene Cymek, Antje Christine Venjakob, Stefan Ruff, Otto Hans-Martin Lutz, Simon Hofmann, and Matthias Roetting. 2014. Entering PIN codes by smooth pursuit eye movements. *Journal of Eye Movement Research* 7(4):1 (2014), 1–11.
- [6] Alexander De Luca, Martin Denzel, and Heinrich Hussmann. 2009. Look into My Eyes!: Can You Guess My Password?. In *Proceedings of the 5th Symposium on Usable Privacy and Security (SOUPS '09)*. ACM, New York, NY, USA, Article 7, 12 pages. DOI : <http://dx.doi.org/10.1145/1572532.1572542>
- [7] Alexander De Luca, Marian Harbach, Emanuel von Zezschwitz, Max-Emanuel Maurer, Bernhard Ewald Slawik, Heinrich Hussmann, and Matthew Smith. 2014. Now You See Me, Now You Don't: Protecting Smartphone Authentication from Shoulder Surfers. In *Proceedings of the 32Nd Annual ACM Conference on Human Factors in Computing Systems (CHI '14)*. ACM, New York, NY, USA, 2937–2946. DOI : <http://dx.doi.org/10.1145/2556288.2557097>
- [8] Alexander De Luca, Roman Weiss, and Heiko Drewes. 2007. Evaluation of Eye-gaze Interaction Methods for Security Enhanced PIN-entry. In *Proceedings of the 19th Australasian Conference on Computer-Human Interaction: Entertaining User Interfaces (OZCHI '07)*. ACM, New York, NY, USA, 199–202. DOI : <http://dx.doi.org/10.1145/1324892.1324932>
- [9] Augusto Esteves, Eduardo Velloso, Andreas Bulling, and Hans Gellersen. 2015. Orbits: Gaze Interaction for Smart Watches Using Smooth Pursuit Eye Movements. In *Proceedings of the 28th Annual ACM Symposium on User Interface Software & Technology (UIST '15)*. ACM, New York, NY, USA, 457–466. DOI : <http://dx.doi.org/10.1145/2807442.2807499>
- [10] Alain Forget, Sonia Chiasson, and Robert Biddle. 2010. Shoulder-surfing Resistance with Eye-gaze Entry in Cued-recall Graphical Passwords. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '10)*. ACM, New York, NY, USA, 1107–1110. DOI : <http://dx.doi.org/10.1145/1753326.1753491>

- [11] Jan Gugenheimer, Alexander De Luca, Hayato Hess, Stefan Karg, Dennis Wolf, and Enrico Rukzio. 2015. ColorSnakes: Using Colored Decoys to Secure Authentication in Sensitive Contexts. In *Proceedings of the 17th International Conference on Human-Computer Interaction with Mobile Devices and Services (MobileHCI '15)*. ACM, New York, NY, USA, 274–283. DOI : <http://dx.doi.org/10.1145/2785830.2785834>
- [12] Oliver Hohlfeld, André Pomp, Jó Ágila Bitsch Link, and Dennis Guse. 2015. On the Applicability of Computer Vision Based Gaze Tracking in Mobile Scenarios. In *Proceedings of the 17th International Conference on Human-Computer Interaction with Mobile Devices and Services (MobileHCI '15)*. ACM, New York, NY, USA, 427–434. DOI : <http://dx.doi.org/10.1145/2785830.2785869>
- [13] Corey Holland, Atenas Garza, Elena Kurtova, Jose Cruz, and Oleg Komogortsev. 2013. Usability Evaluation of Eye Tracking on an Unmodified Common Tablet. In *CHI '13 Extended Abstracts on Human Factors in Computing Systems (CHI EA '13)*. ACM, New York, NY, USA, 295–300. DOI : <http://dx.doi.org/10.1145/2468356.2468409>
- [14] Corey Holland and Oleg Komogortsev. 2012. Eye Tracking on Unmodified Common Tablets: Challenges and Solutions. In *Proceedings of the Symposium on Eye Tracking Research and Applications (ETRA '12)*. ACM, New York, NY, USA, 277–280. DOI : <http://dx.doi.org/10.1145/2168556.2168615>
- [15] Mohamed Khamis, Florian Alt, and Andreas Bulling. 2015. A Field Study on Spontaneous Gaze-based Interaction with a Public Display Using Pursuits. In *Adjunct Proceedings of the 2015 ACM International Joint Conference on Pervasive and Ubiquitous Computing and Proceedings of the 2015 ACM International Symposium on Wearable Computers (UbiComp/ISWC'15 Adjunct)*. ACM, New York, NY, USA, 863–872. DOI : <http://dx.doi.org/10.1145/2800835.2804335>
- [16] Manu Kumar, Tal Garfinkel, Dan Boneh, and Terry Winograd. 2007. Reducing Shoulder-surfing by Using Gaze-based Password Entry. In *Proceedings of the 3rd Symposium on Usable Privacy and Security (SOUPS '07)*. ACM, New York, NY, USA, 13–19. DOI : <http://dx.doi.org/10.1145/1280680.1280683>
- [17] Dachuan Liu, Bo Dong, Xing Gao, and Haining Wang. 2015. Exploiting Eye Tracking for Smartphone Authentication. In *Proceedings of the 13th International Conference on Applied Cryptography and Network Security (ACNS '15)*. 20.
- [18] Päivi Majaranta and Andreas Bulling. 2014. *Eye Tracking and Eye-Based Human-Computer Interaction*. Springer London, 39–65. DOI : http://dx.doi.org/10.1007/978-1-4471-6392-3_3
- [19] Stefan Schneegass, Frank Steimle, Andreas Bulling, Florian Alt, and Albrecht Schmidt. 2014. Smudge-Safe: Geometric Image Transformations for Smudge-resistant User Authentication. In *Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing (UbiComp '14)*. ACM, New York, NY, USA, 775–786. DOI : <http://dx.doi.org/10.1145/2632048.2636090>
- [20] Furkan Tari, A. Ant Ozok, and Stephen H. Holden. 2006. A Comparison of Perceived and Real Shoulder-surfing Risks Between Alphanumeric and Graphical Passwords. In *Proceedings of the Second Symposium on Usable Privacy and Security (SOUPS '06)*. ACM, New York, NY, USA, 56–66. DOI : <http://dx.doi.org/10.1145/1143120.1143128>

- [21] Vytautas Vaitukaitis and Andreas Bulling. 2012. Eye Gesture Recognition on Portable Devices. In *Proceedings of the 2012 ACM Conference on Ubiquitous Computing (UbiComp '12)*. ACM, New York, NY, USA, 711–714. DOI : <http://dx.doi.org/10.1145/2370216.2370370>
- [22] Mélodie Vidal, Andreas Bulling, and Hans Gellersen. 2013. Pursuits: Spontaneous Interaction with Displays Based on Smooth Pursuit Eye Movement and Moving Targets. In *Proceedings of the 2013 ACM International Joint Conference on Pervasive and Ubiquitous Computing (UbiComp '13)*. ACM, New York, NY, USA, 439–448. DOI : <http://dx.doi.org/10.1145/2493432.2493477>
- [23] Mélodie Vidal, Andreas Bulling, and Hans Gellersen. 2015. Pursuits: Spontaneous Eye-Based Interaction for Dynamic Interfaces. *GetMobile: Mobile Comp. and Comm.* 18, 4 (Jan. 2015), 8–10. DOI : <http://dx.doi.org/10.1145/2721914.2721917>
- [24] Paul Viola and MichaelJ. Jones. 2004. Robust Real-Time Face Detection. *International Journal of Computer Vision* 57, 2 (2004), 137–154. DOI : <http://dx.doi.org/10.1023/B:VISI.0000013087.49260.fb>
- [25] Emanuel von Zezschwitz, Alexander De Luca, Bruno Brunkow, and Heinrich Hussmann. 2015. SwiPIN: Fast and Secure PIN-Entry on Smartphones. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems (CHI '15)*. ACM, New York, NY, USA, 1403–1406. DOI : <http://dx.doi.org/10.1145/2702123.2702212>
- [26] Emanuel von Zezschwitz, Paul Dunphy, and Alexander De Luca. 2013. Patterns in the Wild: A Field Study of the Usability of Pattern and Pin-based Authentication on Mobile Devices. In *Proceedings of the 15th International Conference on Human-computer Interaction with Mobile Devices and Services (Mobile-HCI '13)*. ACM, New York, NY, USA, 261–270. DOI : <http://dx.doi.org/10.1145/2493190.2493231>
- [27] Erroll Wood and Andreas Bulling. 2014. EyeTab: Model-based Gaze Estimation on Unmodified Tablet Computers. In *Proceedings of the Symposium on Eye Tracking Research and Applications (ETRA '14)*. ACM, New York, NY, USA, 207–210. DOI : <http://dx.doi.org/10.1145/2578153.2578185>
- [28] Yanxia Zhang, Andreas Bulling, and Hans Gellersen. 2014. Pupil-canthy-ratio: a calibration-free method for tracking horizontal gaze direction. In *Proc. of the 2014 International Working Conference on Advanced Visual Interfaces (AVI 14)*. ACM, New York, NY, USA, 129–132. <http://dx.doi.org/10.1145/2598153.2598186>